

UNITED STATES DISTRICT COURT

for the
Middle District of Alabama

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with Google accounts listed in
Attachment A that are stored at premises controlled by
Google, Inc.

Case No. 2:17mj30-TFM

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Middle District of Alabama, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

Title 18 U.S.C. § 1591

Sex trafficking of children or by force, fraud, or coercion.

The application is based on these facts:

See Affidavit.

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 365 days (give exact ending date if more than 30 days: 02/09/2018) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

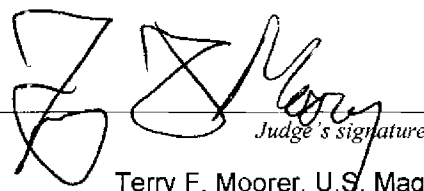
David M. Chamberlin, SA, DHS/Homeland Sec. Inv.

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/09/2017

City and state: Montgomery, AL


Judge's signature

Terry F. Moorer, U.S. Magistrate Judge

Printed name and title

**UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION**

IN THE MATTER OF THE APPLICATION OF)
THE UNITED STATES OF AMERICA FOR A)
SEARCH WARRANT FOR INFORMATION)
ASSOCIATED WITH GOOGLE ACCOUNTS)
LISTED IN ATTACHMENT A THAT ARE)
STORED AT PREMISES CONTROLLED BY)
GOOGLE, INC.)

Case No. 2:17mj-30-TFM

UNDER SEAL

AFFIDAVIT FOR SEARCH WARRANT

I, David M. Chamberlin, Special Agent with the Department of Homeland Security,
Homeland Security Investigations, being duly sworn, hereby deposes and states as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent (SA) with the Department of Homeland Security, Homeland Security Investigations (HSI) since October 2009, and I am currently assigned to the Post of Duty office in Montgomery, Alabama (AL). I currently investigate federal violations concerning human trafficking, child pornography, and the sexual exploitation of children. I have gained experience through training in seminars, classes, and daily work related to these types of investigations. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information.

2. As a federal agent, I am authorized to investigate violations of the laws of the United States, and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. This Affidavit is made in support of an application for a search warrant for information associated with the Google account identified by the following user name, listed in Attachment A, which is stored at the premises owned, maintained, controlled, or operated by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA 94043:

a. josh.rose.jr01@gmail.com

A preservation letter was sent regarding this account on December 23, 2016.

4. I am requesting authority to search the Google accounts where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

5. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause that evidence, fruits, and instrumentalities of the violations of 18 U.S.C. § 1591 (sex trafficking of children or by force, fraud, or coercion) are presently located within the Google accounts listed in Attachment A. Where statements of others are set forth in this Affidavit, they are set forth in substance and in part.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

RELEVANT BACKGROUND INFORMATION

GOOGLE SERVICES

7. Based on my training and experience, as well as conversations with other law enforcement agents, I know the following regarding Google:

- a. Google provides a variety of online services, including electronic mail (“email”) access, to the public. Google allows subscribers to obtain email accounts at the domain name “gmail.com,” like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google ask subscribers to provide basic personal information which those providers retain as associated with the email account. They also retain certain other information associated with the email account, such as account access information and email transactional information. The email account can be used to create, transmit, receive, and store content. This content may include both retrieved and un-retrieved email. Google’s computer servers are therefore likely to contain stored electronic communications, including retrieved and un-retrieved email, and information concerning subscribers and their use of each provider’s services, such as account access information, email transaction information, and account application information. From my training and experience, I know that such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.
- b. In general, an e-mail that is sent to a Gmail subscriber is stored in the subscriber’s “mail box” on Google Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google Inc.’s servers indefinitely. The user can move and store messages in personal folders such as a “sent folder.” In recent years, Google Inc., and other ISPs have provided their users with larger storage capabilities associated with the user’s e-mail account. Google Inc., and other ISPs have allowed users to store up to one (1) terabyte of information associated with the account on ISP servers. Based on conversations with other law enforcement officers with experience in executing and reviewing search warrants of e-mail accounts, I have learned that search warrants for e-mail accounts and computer systems have revealed stored e-mails sent and/or received many years prior to the date of the search.
- c. A sent or received e-mail typically includes the content of the message (including attachments), source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message

may also be saved by Google Inc. but may not include all of these categories of data.

- d. A Google subscriber can also use various Google online services, including Picasa and Google Drive, to archive or store files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (including ones not attached to emails) and other files on servers maintained and/or owned by Google. From my training and experience, and conversations with other law enforcement officers, I know that evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files. I also know, from my training and experience, that evidence of who was using an email account may be found in online archiving or cloud storage services, such as Google's Picasa service (online photo storage and sharing service), and Google Drive (online cloud storage), linked to or associated with a particular Google email account. In fact, I am aware that Google markets its Gmail service in part by encouraging users to archive instead of deleting messages. Archived messages remain accessible to the user, while permanently deleted messages do not.
- e. The mobile number and alternate e-mail information provided to Google Inc., by the user are particularly useful in instances where a user needs to recover his/her account in the event of a lost password or account compromise. With these, Google Inc. can send a "reset password" link to the alternate e-mail address, or an SMS message to the mobile number. Upon receiving the "reset password" link to an SMS mobile number affiliated with that account, the user can then reset the password in order to continue to utilize that particular account. Because both a mobile device number and alternate e-mail address are used to recover access to an account, they both tend to be closely associated with the user of the account. It is important to note that though Google Inc. attempts to validate the personal identifying information provided by subscribers, the validation requires additional voluntary input from users. As this additional input is voluntary, Google Inc. is not always successful in validating a user's personal identifying information.
- f. Based on my training and experience, and conversations with other law enforcement officers, I know that email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP

address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

- g. When creating an account at Google Inc., the user is provided the opportunity to create a display name and an associated “Profile.” Google Inc. allows a user to personalize their Profile by “adding an image that represents you.” The display name and display image a user provides for their Profile is public and can be seen by anyone, even if the user chooses to keep the rest of their Profile hidden from other users.
- h. From my training and experience, and conversations with other law enforcement officers, I know that in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications. From my training and experience, and conversations with other law enforcement officers, I know that such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.
- i. In my training and experience, I have also learned that Google Inc. provides an on-line service called Google Messenger to the general public. Google Messenger is an instant messaging client provided by Google. Instant Messaging (“IM”) is a form of real-time direct text-based communication between two or more people using shared clients. The text is conveyed via devices connected over a network such as the Internet. Google also allows users versions to utilize its webcam service. This option enables users from distances all over the world to view others who have installed a webcam on their end. In order to obtain a Google Messenger account, a Google email account is required. The Google email user must download the Google Messenger program and sign in with the same credentials used for his/her Google email account. The Terms of Service notify the user that Google Messenger will allow the user and the people the user communicates with to save those conversations and other information into the user’s affiliated Google email account. Google Messenger also allows users to exchange computer to computer voice calls with their online contacts. If a user subscribes to the “Phone In” or “Phone Out” premium services, the user can also use Google Messenger to make or receive calls from regular telephones.

- j. A user may archive Google instant messages along with Google email messages and search them together (in addition to Voice Mail, SMS, call history, and more). For users that have elected to archive their messages, Google Messenger will now archive messages on Google servers to establish and maintain this archive. Messages stored on Google servers in this manner are accessible from any computer system or device able to use the latest versions of Google Messenger for computer. Users can view their Google Messenger conversation history and Google email archive (if they are tied to the same user ID) on Google Messenger through “Conversation History” in the settings. A user can turn off this feature for instant messages at any time by selecting “Do not keep a record of my conversations.” Even if a user chooses not to save his message history, users with whom he communicates may opt to use the functionality available in their version of Google Messenger to save the communications and his conversations may be saved on Google servers, just like e-mail. Users can delete their archived messages by selecting the message, and clicking on the “Delete” button. However, this does not delete any of their conversations saved by other users.

- k. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored in the user’s account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Lastly, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime

(e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

1. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.^a

PROBABLE CAUSE

8. On July 20, 2016, HSI received information regarding the investigation by the Prattville, Alabama Police Department regarding an individual named Joshua ROSE (hereinafter "ROSE") for the prostitution of several women, including possible juvenile victims. On June 7, 2016, Investigator Jason Hamm with the Prattville Police Department (PPD) received a phone call from Victim 1. Victim 1, an adult, informed Investigator Hamm that ROSE had been forcing her, along with another adult victim (Victim 2), and "four or five" juveniles, including Victim 3, to have sex for money at the Stay Lodge hotel in Montgomery, Alabama.

9. PPD investigators interviewed Victim 1 on June 7, 2016; July 22, 2016; and July 28, 2016. Victim 1 stated that ROSE forced her to perform sex with men for money.

^a It is possible that Google stores some portion of the information sought outside of the United States. In *Microsoft Corp. v. United States*, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information—including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Google. The government also seeks the disclosure of the physical location or locations where the information is stored.

Victim 1 stated that ROSE posted an advertisement with her photographs on Backpage.com. She stated that ROSE took the photo of her to be used for Backpage.com. She stated that ROSE picked the clothing she wore and the manner in which she posed for the photos to be used for Backpage.com. Victim 1 stated that ROSE would arrange for men to have sex with his victims at, among other places, the Stay Lodge hotel, the Red Roof Inn, and a trailer where ROSE lived. Victim 1 identified the Google email addresses josh.rose.jr01@gmail.com and rose.pimpin69@gmail.com as being used by ROSE, as well as identifying additional phone numbers used by ROSE.

10. PPD investigators interviewed Victim 2 on September 13, 2016; September 14, 2016; and October 6, 2016. Victim 2 also provided PPD with a written statement. Victim 2 stated that ROSE made her have sex with men for money. Victim 2 stated that ROSE took a picture of her with Victim 1, but was unaware that it was used for an advertisement on Backpage.com.

11. PPD investigators interviewed Victim 3 on June 13, 2016; July 22, 2016; and July 28, 2016. Victim 3 stated that ROSE made her have sex in exchange for money at the Stay Lodge hotel in Montgomery, Alabama. Victim 3 stated that ROSE posted an advertisement for her on Backpage.com. When shown advertisements from Backpage.com found online by PPD, Victim 3 identified herself as the subject in the images of the advertisement. Victim 3 stated that ROSE would become violent and that she was scared of him. Victim 3 stated that during an approximately three-day stay at the Stay Lodge, ROSE made her have sex with five men.

12. PPD Investigators located several advertisements posted on Backpage.com featuring individuals later identified as Victims 1 and 2. For example, one advertisement located by PPD was posted to Backpage.com on May 24, 2016. It featured four photographs of an

individual later identified to be Victim 3 posed on what appears to be a bed. The caption reads “Just turned 18 freaky toy – 18.” The phone number listed in the advertisement is xxx-xxx-3202, determined to belong to ROSE.

13. Backpage.com is an online forum for classified advertisements. *See generally Backpage.com, LLC v. Dart*, 807 F.3d 229, 230 (7th Cir. 2015). It includes an “adult” section that includes subcategories, such as “escorts, body rubs, strippers and strip clubs, dom[ination] and fetish, ts (transsexual escorts), male escorts, phone [sex], and adult jobs.” *Id.* Courts have recognized that the majority of these advertisements are, in fact, advertisements for sex. *Id.* To post an advertisement on Backpage.com, a user must first create an account. Creating an account requires the use of an email address. *See generally* www.my.backpage.com.

14. On June 10, 2016, Investigator Hamm subpoenaed Backpage.com, requesting any and all records pertaining to the phone number xxx-xxx-3202. The response from Backpage.com included account information linking that phone number to a post advertising prostitution. Attached to the post were several images of what appeared to be Victim 3.

15. On July 21, 2016, PPD investigators issued a subpoena to Backpage.com for any and all records pertaining to email address josh.rose.jr01@gmail.com, believed to belong to ROSE. The response from Backpage.com included several advertisements listed using the email address josh.rose.jr01@gmail.com. For example, one advertisement posted using that email address depicts three photos of a female whose face is not visible. In the first photo, she is wearing only a pair of shorts, and her breasts are covered by her hands. In the second photo, she is wearing shorts and a gray sports bra. In the third photo, she is wearing shorts but no shirt or bra, and she is kneeling on what appears to be a bed with her chest on the bed and her buttocks in the air. The caption for the advertisement is “Sexy little toy – 18.” Further text in the

advertisement states, “I finally turned 18 last month, now daddy can’t tell me what to do...but you can let me be your fantasy call or text [xxx]-[xxx]-3202 I’m very tight btw.” The phone number listed is xxx-xxx-3202, which, as stated above, was determined through this investigation to belong to ROSE. Victim 3, a minor, identified herself in two of the photos attached to this advertisement.

16. On July 27, 2016, PPD investigators issued a subpoena to Backpage.com for any and all records pertaining to email address rose.pimpin69@gmail.com, believed to belong to ROSE. In the response, that subpoena indicated that Backpage.com could not locate any records containing that email address.

17. Based on the above, there is probable cause to believe that the contents of the Google email address josh.rose.jr01@gmail.com contains evidence, fruits, and instrumentalities related to the sex trafficking of children or by force, fraud, or coercion in violation of 18 U.S.C. § 1591.

18. Furthermore, as explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each offense-element, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how

and when the account was accessed or used. For example, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Finally, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

19. In my training and experience, e-mail users often use e-mail accounts for everyday transactions because it is fast, low cost, and simple to use. People use e-mail to communicate with friends and family, manage accounts, pay bills, and conduct other online business. E-mail users often keep records of these transactions in their e-mail accounts, to include personal identifying information, such as name and address.

REQUEST FOR PRECLUDING NOTICE

20. It is respectfully requested, pursuant to 18 U.S.C. § 2705(b), that Google be ordered not to disclose the existence or service of the search and seizure warrant to the subscriber, customer, or any other person, for a period of one year from the date of said order (unless that period is extended by further order of the Court), except as required to disclose to

Google's officers, employees, or agents to the extent necessary to comply with the warrant. Based upon my knowledge, training, and experience, it is my belief that notification at this time of the existence of the warrant will result in the destruction of or tampering with evidence, and otherwise seriously jeopardize an investigation.

REQUEST FOR SEALING

21. I further request that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this Affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may cause the destruction of or tampering with evidence and otherwise seriously jeopardize an investigation. Premature disclosure of the contents of the application, this Affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

EXECUTION OF THE WARRANT

22. If approved, I anticipate executing this search warrant under the Electronic Communications Privacy Act – Title 18, United States Code, Sections 2703(a) and 2703(b)(1)(A), by using the warrant to require Google, Inc., to disclose copies of the records and information (including content of communications) as described particularly in Attachment A. Upon receipt of the information described in Attachment A, authorized persons will review the information in order to locate the items described in Attachment B.

23. Based upon my training and experience, I understand that Google, Inc., requires a court order before it will provide responsive data that may include child pornography. I,


therefore, request that the Court order Google, Inc., to disclose data responsive to this search warrant, notwithstanding 18 U.S.C. § 2252A or similar statute.

CONCLUSION

24. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the following criminal offenses may be located in the accounts described in Attachment A, that is stored at premises owned, maintained, controlled or operated by Google, Inc., an online services company which currently accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA 94043: sex trafficking of children or by force, fraud, or coercion, in violation of 18 U.S.C. § 1591.

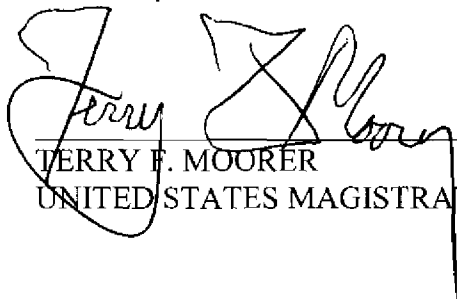
25. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

26. Because the warrants for the accounts described in Attachment A will be served on Google, Inc., who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.



David M. Chamberlain
Special Agent
Homeland Security Investigations

Sworn to and subscribed to before me
this 7th day of February, 2017. 0900



TERRY F. MOORER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with the account josh.rose.jr01@gmail.com that is stored at premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

**Particular Things to be Seized and Procedures
to Facilitate Execution of the Warrant**

I. Information to be disclosed by Google, Inc. (the “Provider”) to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to the request made under 18 U.S.C. § 2703(f) on December 23, 2016, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, e-mail attachments, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information, including address books, contact and buddy lists, calendar data, pictures, and files; and
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

Google, Inc. shall disclose responsive data, if any, by sending to 1064 Monticello Park, Montgomery, Alabama 36117 using the U.S. Postal Service or another courier service, notwithstanding 18 U.S.C. § 2255A or similar statute or code.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2422(b) and 3261(a), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Any person persuading, inducing, enticing, and/or coercing a minor to engage in an illegal sexual act with an adult;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the criminal activity under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s); and
- (e) Identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses.

III. Government procedures for warrant execution

The United States government will conduct a search of the information produced by the Provider and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the Provider that does not fall within the scope of Section II and will not further review the information absent an order of the Court.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and
- c. such records were made by Google, Inc., as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature